Европейски парламент
2014-2019

Документ за разглеждане в заседание

B8-0153/2019

6.3.2019

ПРЕДЛОЖЕНИЕ ЗА РЕЗОЛЮЦИЯ

за приключване на разисквания по изявления на Съвета и на Комисията

съгласно член 123, параграф 2 от Правилника за дейността

относно заплахите за сигурността във връзка със засилващото се технологично присъствие на Китай в ЕС и възможни действия на равнището на ЕС за ограничаването им
(2019/2575(RSP))

Тициана Бегин, Дарио Тамбурано, Изабела Адинолфи, Роландас Паксас
от името на групата EFDD

B8-0153/2019

Резолюция на Европейския парламент относно заплахите за сигурността във връзка със засилващото се технологично присъствие на Китай в ЕС и възможни действия на равнището на ЕС за ограничаването им
(2019/2575(RSP))

Европейският парламент,

– като взе предвид съобщенията на Комисията от 14 септември 2016 г., озаглавени „Свързаност за изграждане на конкурентоспособен цифров единен пазар – към европейско общество на гигабитов интернет“ (COM(2016)0587) и „5G за Европа: план за действие“ (COM(2016)0588),

– като взе предвид измененото предложение на Комисията за регламент на Европейския парламент и на Съвета от 29 януари 2016 г. относно достъпа на стоки и услуги от трети държави до вътрешния пазар на обществени поръчки на Съюза и за определяне на процедурите за подпомагане на преговорите относно достъпа на съюзни стоки и услуги до пазарите на обществени поръчки на трети държави (COM(2016)0034),

– като взе предвид Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза[1] (Директивата за мрежова и информационна сигурност),

– като взе предвид предложението от 13 септември 2017 г. за регламент на Европейския парламент и на Съвета относно ENISA – Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“) (COM(2017)0477),

– като взе предвид Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения[2],

– като взе предвид предложението на Комисията от 12 септември 2018 г. за регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове (COM(2018)0630),

– като взе предвид процедурата на СТО за уреждане на спорове (WT/DS549/6) от 1 юни 2018 г. относно някои мерки, наложени от Китай, във връзка с трансфера на чуждестранни технологии в Китай,

[1] ОВ L 194, 19.7.2016 г., стр. 1.
[2] ОВ L 321, 17.12.2018 г., стр. 36.

– като взе предвид своята позиция, приета на първо четене на 14 февруари 2019 г., относно предложението за регламент на Европейския парламент и на Съвета за създаване на рамка за скрининг на преки чуждестранни инвестиции в Европейския съюз[3],

– като взе предвид текущите преговори между ЕС и Китай за сключването на всеобхватно споразумение за инвестиции,

– като взе предвид член 123, параграф 2 от своя правилник,

А. като има предвид, че неотдавнашният напредък на информационните и комуникационните технологии (ИКТ), включително телекомуникациите от пето поколение (5G), проправиха пътя за производството, разпространението и ползването на стоки и услуги, както и за взаимодействията между устройствата и между гражданите, публичната администрация и други социално-икономически участници, с което биха могли да дадат тласък на европейската икономика;

Б. като има предвид, че киберсигурността в областта на ИКТ, защитата на чувствителната информация, зачитането на индивидуалните права и защитата от външни киберзаплахи са предварително условие за обезпечаването на технологичния суверенитет на гражданите на ЕС и в крайна сметка – за осигуряването на просперитет и подкрепа за демокрацията в ЕС;

В. като има предвид, че изследванията и изпитванията в областта на 5G едва успяват да отговорят на международния натиск за развитие и предлагане на пазара на 5G, а редица научни изследвания породиха загриженост и съмнения по отношение на тяхната сигурност и безопасност, особено във връзка с риска от електромагнитно замърсяване за човешкото здраве и околната среда;

Г. като има предвид, че киберсигурността на мрежите от пето поколение е ново и сложно предизвикателство поради техния виртуален и децентрализиран характер и тяхната фрагментирана и високоспециализирана верига на стойността, от производството до доставката, инсталирането, конфигурирането, функционирането, поддръжката и софтуерните актуализации; като има предвид, че ЕС трябва да отстрани пропуските в киберсигурността в своята критична инфраструктура, наред с другото в секторите на далекосъобщенията, енергетиката, транспорта, здравеопазването, отбраната и сигурността;

Д. като има предвид, че осигуряването на безопасни и сигурни мрежи от пето поколение е задача, която не може да бъде изпълнена от отделните производители или системни оператори, а изисква ефективни координирани действия от всички имащи отношение национални и международни органи;

Е. като има предвид, че ЕС е способен да води развитието на технологиите за киберсигурност, като подкрепя европейските предприятия в този сектор и насърчава всички промени във веригата на стойността, които биха могли да намалят зависимостта на ЕС от чуждестранни технологии;

[3] Приети текстове, P8_TA(2019)0121.

Ж. като има предвид, че ЕС разработва набор от мерки за гарантиране на киберсигурността, в т.ч. Директивата за мрежова и информационна сигурност и Акта за киберсигурността, които следва да бъдат приложени бързо и да бъдат под непрекъснато наблюдение, за да се гарантира, че продължават да бъдат ефективни и след необходимите актуализации и прегледи;

З. като има предвид, че засиленото присъствие на технологии от Китай и от други трети държави е вече очевидно на пазара на ЕС на 5G, особено в държавните предприятия или в предприятията, които не осигуряват достатъчно прозрачност;

И. като има предвид, че взаимността е един от най-ефективните начини за постигане на напредък към еднакви условия на конкуренция в световен мащаб;

Й. като има предвид, че чуждестранните дружества трябва да се справят в настоящите несъответствия в стандартите на ЕС за защита на данните между Общия регламент относно защитата на данните и различните изисквания съгласно националните закони;

К. като има предвид, че от 2013 г. ЕС и Китай водят преговори за сключването на всеобхватно споразумение за инвестиции; като има предвид, че предложената сделка ще спомогне за решаването на въпроси във връзка с достъпа до пазара, ще установи рамка за защита на инвестициите и ще определи основни трудови и екологични стандарти;

Л. като има предвид, че макар да не е окончателно потвърдено, по отношение на пропуските в сигурността на оборудването, доставяно от доставчици от трети държави, в т.ч. Китай, стана ясно, че те биха могли да застрашат индивидуалните права на неприкосновеност на личния живот и защитата на чувствителна информация в ЕС;

1. подчертава, че внедряването и предлагането на пазара на 5G следва да се осъществява в съответствие с принципа на предпазните мерки, като всички социално-икономически участници анализират предварително възможните последици за безопасността и сигурността и вземат пропорционални предпазни мерки, включително бързо разкриване на фактори, които биха могли да застрашат общественото здраве или околната среда;

2. подчертава, че социалното и икономическото въздействие на 5G и на технологиите, които прави възможни, от интернет на нещата до изкуствения интелект, следва да бъдат подложени на задълбочена оценка и че следва да бъдат взети мерки с цел преход към европейско общество на гигабитов интернет, който да се осъществи съобразно справедливи и равни условия за всички и на основата на етична отговорност;

3. призовава Комисията и държавите членки да създадат благоприятна за иновациите среда за доставчиците от ЕС за разработването на нови продукти, услуги и технологии и да подкрепят предприемачеството в ЕС в областта на внедряването и предлагането на пазара на безопасни и сигурни 5G, като същевременно гарантират, че техният потенциал е достъпен за всички предприятия от сектора на цифровата икономика в ЕС, включително малките и

средните предприятия;

4. припомня, че киберсигурността е едно от основните предизвикателства, пред които е изправен понастоящем ЕС, и че неуспехът в тази област би могъл да означава нарушение на неприкосновеността на личния живот и на основните права на потребителите и производителите от ЕС, сериозно да подкопае доверието на гражданите в продуктите и услугите на ИКТ и в крайна сметка да нанесе тежки икономически вреди; призовава за мрежа, която е сигурна по подразбиране и още от етапа на проектиране;

5. призовава Комисията и държавите членки да си сътрудничат тясно при прилагането на стратегията на ЕС за киберсигурност и да съчетават мерки на ЕС и национални мерки с цел да се сведе до минимум рискът от пропуски в сигурността и от нарушения на сигурността на данните по цялата верига на стойността; счита, че подобни мерки биха могли да включват сертифициране на киберсигурността в ЕС, изисквания относно конфигурацията и оперативни процедури и практики, както и насърчаване на киберхигиена и цифровото образование;

6. счита, че ролята на агенцията на ЕС по киберсигурност (Агенцията на Европейския съюз за мрежова и информационна сигурност – ENISA) е от решаващо значение за анализа на възможните заплахи, пораждани от чуждестранните доставчици, включително Китай, и за координираното прилагане от страна на държавите членки на общ подход за справяне със заплахите и атаките, насочени срещу киберсигурността;

7. призовава Комисията и държавите членки да приложат бързо пакета в областта на кръговата икономика и да усъвършенстват управлението на суровините през целия им жизнен цикъл, както и рециклирането на отпадъците, така че да се подобри достъпът на ЕС до суровини от изключителна важност, които са от първостепенно значение за високотехнологичните продукти и най-новите иновации;

8. счита, че е належащо да се преодолеят възможните заплахи за технологичната сигурност, които поставя текущото навлизане на пазара на ЕС на чуждестранни доставчици, включително Китай, като се възприеме от страна на държавите членки общ подход по отношение на сигурността и защитата на данните;

9. призовава Комисията и държавите членки да анализират и наблюдават сигурността на ИКТ системите, в които се отчита силно присъствие на технологии от трети държави, в т.ч. чрез провеждането на стрес тестове;

10. подчертава, че доставчиците от трети държави не следва да бъдат дискриминирани на основа на тяхната държава на произход, но че прозрачността на тези дружества, техните стандарти за киберсигурност и съществуването на взаимни условия за европейските дружества в държавата на произход следва да бъдат вземани предвид, за да се осигурят еднакви условия на конкуренция;

11. подчертава, че при никакви обстоятелства доставчиците и операторите от Китай или от други трети държави не следва да застрашават индивидуалните права,

гарантирани от правото на ЕС, дори при наличието на различни изисквания съгласно националното право в тяхната държава на произход;

12. изисква Съветът да разгледа с положително отношение възможността за възобновяване на разискванията по новото преразгледано предложение на Комисията относно процедурата на ограничаване на достъпа на чуждестранни продукти до пазара на ЕС на обществени поръчки, когато не се предоставя ответен достъп;

13. припомня значението на по-нататъшното подобряване на преговорите относно регулаторното сътрудничество с трети държави в областта на цифровите технологии и на гарантирането на по-силен ангажимент от тяхна страна в международните органи по стандартизация;

14. възлага на своя председател да предаде настоящата резолюция на Съвета и на Комисията.